PATENT
Atty. Dkt. No. 2000-0415

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:
Aviel D. Rubin

Serial No.: 09/682,526

Confirmation No.: 3764

Filed: September 14, 2001

For: METHOD FOR SECURE REMOTE BACKUP

Group Art Unit: 2131

Examiner: Arezoo Sherkat

MAIL STOP **APPEAL BRIEF - PATENTS**
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

CERTIFICATE OF MAILING OR TRANSMISSION
I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, or being facsimile transmitted to the USPTO, on the date indicated below.

October 13, 2006
Date

Signature

Dear Sir:

SUPPLEMENTAL APPEAL BRIEF

The following Supplemental Appeal Brief is submitted in response to the Office Action dated July 13, 2006 (Paper No. 20060630) to reinstate the Appeal filed February 17, 2006. The Supplemental Appeal Brief addresses the new grounds for rejection raised by the Examiner after prosecution was reopened following the filing of the original Appeal. A Notice of Appeal was filed and received in the Patent Office on February 17, 2006 in the above-identified application. A second Notice of Appeal dated October 13, 2006 is enclosed to reinstate the Appeal.

The Appellant believes that the fees for the Appeal were paid for the Notice of Appeal submitted on February 17, 2006 and the Appeal Brief submitted on April 17, 2006. The Commissioner is hereby authorized to charge counsel's Deposit Account No. 20-0782, for any fees, including the extension of time fees or the difference in fees previously paid for the Notice of Appeal and the Appeal Brief, required to make this response timely and acceptable to the Office.

REAL PARTY IN INTEREST

The real party in interest is AT&T, Corp.

RELATED APPEALS AND INTERFERENCES

The Appellant knows of no related appeals or interferences that might directly affect or be directly affected by or have bearing on the Board's decision in the pending appeal.

STATUS OF CLAIMS

Claims 1-16 are pending in the application. Claims 1-16 were originally presented in the application. Claims 1-16 stand rejected in view of several references as discussed below. The rejection of claims 1-16 based on the cited references is appealed. The pending claims are shown in the attached Appendix.

STATUS OF AMENDMENTS

Claims 5 and 13 were amended in a response to an Office Action dated August 2, 2004, filed on December 2, 2004, to correct informalities. No amendments to the claims, in this application, were submitted subsequent to final rejection. The Appellant is appealing the claims as they read at the time the final rejection was issued. These claims are shown in the attached Appendix.

SUMMARY OF CLAIMED SUBJECT MATTER

The present invention provides for a method and device-readable medium storing program instructions pertaining to backing up one or more files on a local device onto remote servers over a network. In the embodiment of independent claim 1, the invention comprises deriving (303) a first cryptographic key and a second cryptographic key from a user-provided passphrase. (See e.g., Appellant's specification, pg. 4, para. [0014].) Then the method compresses (304) one or more files and adds (304) each of the files to a bundle (200). (See *Id.* at pg. 5, para. [0015].) Next, an authentication code (228) for the bundle (200) using the first cryptographic key is generated (306) and the authentication code (228) is added to the bundle (306). (See *Id.*) The method concludes by encrypting (307) the bundle (200) using the second cryptographic key prior to sending the bundle to the remote server. (See *Id.*)

In the embodiment of independent claim 5, a method for restoring one or more files on remote servers to a local device over a network is described. The method comprises deriving (402) a first cryptographic key and a second cryptographic key from a user-provided passphrase. (See e.g., Appellant's specification, page 6, para. [0019].) Then the method decrypts (407) a bundle (200) received from the remote server using the second cryptographic key. (See *Id.*) Next, an authentication code (228) in the bundle (200) is checked (408) using the first cryptographic key. (See *Id.*) The method concludes by decompressing (409) one or more files from the bundle (200). (See *Id.*)

In the embodiment of independent claim 9, a device-readable medium storing program instructions for performing a method of backing up one or more files on a local device onto remote servers over a network is described. The program instructions for the method stored on the device-readable medium comprises deriving (303) a first cryptographic key and a second cryptographic key from a user-provided passphrase. (See e.g., Appellant's specification, pg. 4, para. [0014].) Then the method compresses (304) one or more files and adds (304) each of the files to a bundle (200). (See *Id.* at pg. 5, para. [0015].) Next, an authentication code (228) for the bundle (200) using the first cryptographic key is generated (306) and the authentication code (228) is added to the bundle (306). (See *Id.*) The method concludes by encrypting (307) the bundle (200) using the second cryptographic key prior to sending the bundle to the remote server. (See *Id.*)

In the embodiment of independent claim 13, a device-readable medium storing program instructions for performing a method of restoring one or more files on remote servers to a local device over a network is described. The program instructions for the method stored on the device-readable medium comprises deriving (402) a first cryptographic key and a second cryptographic key from a user-provided passphrase. (See e.g., Appellant's specification, page 6, para. [0019].) Then the method decrypts (407) a bundle (200) received from the remote server using the second cryptographic key. (See *Id.*) Next, an authentication code (228) in the bundle (200) is checked (408) using the first cryptographic key. (See *Id.*) The method concludes by decompressing (409) one or more files from the bundle (200). (See *Id.*)

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-3, 5-7, 9-11 and 13-15 stand rejected under 35 U.S.C. §103(a) as being obvious over Bailey, III (U.S. Patent 5,659,614, issued August 19, 1997, hereinafter referred to as "Bailey") in view of Matyas Jr., et al. (U.S. Patent 7,010,689, issued March 7, 2006, hereinafter referred to as "Matyas I"). Claims 4, 8, 12 and 16 stand rejected under 35 U.S.C. §103(a) as being obvious over Bailey in view of Matyas I in further view of Matyas, et al. (US Patent 5,201,000, issued April 6, 1993, hereinafter referred to as "Matyas II").

ARGUMENT

A. 35 U.S.C. §103(a) – Bailey in view of Matyas I

1. Claim 1

The Examiner has rejected claim 1 in the Office Action under 35 U.S.C. §103 as being unpatentable over Bailey in view of Matyas I. Appellant respectfully traverses the rejection.

Bailey teaches a method and system for creating and storing a backup copy of file data stored on a computer. "The file data to be backed up is encrypted using multiple, indirect encryption keys, variable block lengths, and variable algorithms based on a client-selected string of characters. The files are thereafter encrypted again at the client site prior to transmission to the backup site. A program registry is maintained at the backup site that contains a master copy of many commercially-available files. The incoming files received from the client site are compared to the files in the program registry. If an incoming file is located in the registry, the file is replaced by a token identifying the commercially-available file and the token is stored at the backup facility." (See Bailey, Abstract.)

Matyas I teaches secure data storage and retrieval in a client-server environment. Matyas teaches an encrypted file that was encrypted with an encryption key ke. (See Matyas I, col. 7, ll. 25-51; FIG. 4). Specifically, a passphrase/password is used to derive a personal key, where the personal key is then used to encrypt the encryption key ke. More specifically, the personal key client also generates a random encryption key ke for encrypting the content of the file. (See Matyas I, col. 9, ll. 14-23, emphasis added).

The Appellant respectfully submits that the combination of Bailey and Matyas I, alone or in any permissible combination, fails to teach or to suggest the novel concept of deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code for a bundle using the first cryptographic key that is ultimately added to and encrypted with the bundle, as positively claimed by the Appellant's independent claim 1. Specifically, Appellant's independent claim 1 positively recites:

> 1. A method of backing up one or more files on a local device onto remote servers over a network comprising:
> deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
> compressing one or more files and adding each of the files to a bundle;
> generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle; and
> encrypting the bundle using the second cryptographic key prior to sending the bundle to the remote server. (Emphasis added.)

In one embodiment, the Appellant's invention provides a method for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle. The derivation step is performed after proactively checking the passphrase for a necessary amount of entropy. (See e.g., Appellant's specification, page 4, para. [0013].) In addition, due to the nature of how the bundle is constructed, the file system structure and the file names are advantageously hidden from the remote server and from anyone listening in on the network. (See *Id.* at page 6, para. [0016].) Consequently, the strong encryption and authentication properties make them tamper evident and opaque to anyone who cannot obtain a user passphrase or break the authentication and encryption files. (See *Id.* at page 7, para. [0020].)

The Appellant respectfully submits that the combination of Bailey and Matyas I, alone or in any permissible combination fails to teach or to suggest a method for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase. Bailey explicitly teaches that "[t]he second encryption is performed by the transmission program based upon internally generated keys." (See Bailey, col. 17, ll. 14-16, emphasis added, see also, Bailey, col. 18, ll. 26-28, "while the second level of encryption is performed by the transmission program that generates its own key.", emphasis added.)

In addition, Bailey states that the client key is derived from a client selected string of characters and the actual encryption key used to encrypt the data is derived from the client key. In other words, the actual encryption key is not generated from the string of characters, but from the client key instead. (See Bailey Column 17, lines 1-5).

Matyas I also fails to bridge the substantial gap left by Bailey because Matyas I teaches creating only one cryptographic key from a user-provided passphrase. (See Matyas I, col. 7, ll. 36-38; col. 9, ll. 15-23.) Unlike the Appellant's invention that teaches deriving a first cryptographic key **and** a second cryptographic key from a user-provided passphrase (i.e. both keys are derived from the user-provided passphrase), Matyas I teaches only one cryptographic key is generated based on a user provided passphrase and the additional cryptographic keys are randomly generated. (See *Id.*) As such, this element in Appellant's claims is completely absent in both references.

Moreover, as indicated by the Examiner on page 4 of the Office Action dated July 13, 2006, Bailey fails to disclose the generation of an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle. However, the Examiner alleges that Matyas I teaches this limitation.

The Appellant respectfully submits that the Examiner has interpreted Matyas I too broadly and must look at Matyas I in its entirety. Matyas I teaches that the personal key client generates a MAC with ki, specifically MAC = Hash(file, ki). (See Matyas I, col. 12, ll. 1-7.) Matyas I further teaches that ki is a randomly generated integrity protection key generated by the personal key client. (See Matyas I, col. 9, ll. 23-30.) Therefore, in Matyas I, the MAC is created using a randomly generated encryption key.

In contrast, the Appellant's invention teaches generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle. In other words, the authentication code is generated using a first cryptographic key that is derived from a user-provided passphrase. Therefore, unlike the Appellant's invention that teaches generating an authentication code using a first cryptographic key that is derived from a user-provided passphrase, Matyas I teaches that the MAC is created using an encryption key that is randomly generated by the personal key client.

Consequently, the Appellant respectfully submits that Bailey and Matyas I, alone or in any permissible combination, fail to teach or to suggest a method for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle, as positively recited by Appellant's independent claim 1. Therefore, the Appellant respectfully submits that independent claim 1 fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

2. Claim 2

Claim 2 stands rejected under 35 U.S.C. §103 as being unpatentable over Bailey in view of Matyas I. Appellant respectfully traverses the rejection.

The Appellant submits that Bailey and Matyas I do not, in any permissible combination, teach, show, or suggest all of the limitations of independent claim 1. Since Bailey and Matyas I do not make obvious the Appellant's invention as recited in Appellant's independent claim 1, dependent claim 2 is also not made obvious since the claim depends directly from claim 1 and recites additional features of the present invention. Thus, claim 2 should be deemed patentable for at least the reasons stated above with respect to independent claim 1.

Secondly, the Appellant contends that the combination of Bailey and Matyas I does not teach the novel concept of a method for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle in combination with encrypting the bundle using a strong block cipher, as set forth in claim 2. Encrypting the bundle with a strong block cipher ensures greater security. This novel approach is absent in the alleged combination of Bailey with Matyas I. Thus, the Appellant respectfully submits that claim 2 is patentable under the provisions of 35 U.S.C. §103.

3. Claim 3

Claim 3 stands rejected under 35 U.S.C. §103 as being unpatentable over Bailey in view of Matyas I. Appellant respectfully traverses the rejection.

The Appellant submits that Bailey and Matyas I do not, in any permissible combination, teach, show, or suggest all of the limitations of independent claim 1. Since Bailey and Matyas I do not make obvious the Appellant's invention as recited in Appellant's independent claim 1, dependent claim 3 is also not made obvious since the claim depends directly from claim 1 and recites additional features of the present invention. Thus, claim 3 should be deemed patentable for at least the reasons stated above with respect to independent claim 1.

Secondly, the Appellant contends that the combination of Bailey and Matyas I does not teach the novel concept of a method for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle in combination with the authentication code being an HMAC, as set forth in claim 3. Using an HMAC as the authentication code ensures greater security. This novel approach is absent in the alleged combination of Bailey with Matyas I. Thus, the Appellant respectfully submits that claim 3 is patentable under the provisions of 35 U.S.C. §103.

4. Claim 5

The Examiner has rejected claim 5 in the Office Action under 35 U.S.C. §103 as being unpatentable over Bailey in view of Matyas I. Appellant respectfully traverses the rejection.

The teachings of Bailey and Matyas I are discussed above.

The Appellant respectfully submits that the combination of Bailey and Matyas I, alone or in any permissible combination, fails to teach or to suggest the novel concept of deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle using the first cryptographic key, as positively claimed by the Appellant's independent claim 5. Specifically, Appellant's independent claim 5 positively recites:

> 5. A method of restoring one or more files on remote servers to a local device over a network comprising:
> deriving a first cryptographic key and a second cryptographic key from a user-provided passphraase;
> decrypting a bundle received from the remote server using the second cryptographic key;
> checking an authentication code in the bundle using the first cryptographic key; and
> decompressing one or more files from the bundle. (Emphasis added.)

In one embodiment, the Appellant's invention provides a method for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle using the first cryptographic key. The derivation step is performed after proactively checking the passphrase for a necessary amount of entropy. (See e.g., Appellant's specification, page 4, para. [0013].) In addition, due to the nature of how the bundle is constructed, the file system structure and the file names are advantageously hidden from the remote server and from anyone listening in on the network. (See *Id.* at page 6, para. [0016].) Consequently, the strong encryption and authentication properties make them tamper evident and opaque to anyone who cannot obtain a user passphrase or break the authentication and encryption files. (See *Id.* at page 7, para. [0020].)

The Appellant respectfully submits that the combination of Bailey and Matyas I, alone or in any permissible combination fails to teach or to suggest a method for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase. Bailey explicitly teaches that "[t]he second encryption is performed by the transmission program based upon internally generated keys." (See Bailey, col. 17, ll. 14-16, emphasis added, see also, Bailey, col. 18, ll. 26-28, "while the second level of encryption is performed by the transmission program that generates its own key.", emphasis added.)

In addition, Bailey states that the client key is derived from a client selected string of characters and the actual encryption key used to encrypt the data is derived from the client key. In other words, the actual encryption key is not generated from the string of characters, but from the client key instead. (See Bailey Column 17, lines 1-5).

Matyas I fails to bridge the substantial gap left by Bailey because Matyas I teaches creating only one cryptographic key from a user-provided passphrase. (See Matyas I, col. 7, ll. 36-38; col. 9, ll. 15-23.) Unlike the Appellant's invention that teaches deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase (i.e. both keys are derived from the user-provided passphrase), Matyas I teaches only one cryptographic key is generated based on a user provided passphrase and the additional cryptographic keys are randomly generated. (See *Id.*) As such, this element in Appellant's claims is completely absent in both references.

Appellant also respectfully submits that the combination of Bailey and Matyas I, alone or in any permissible combination fails to teach or to suggest a method for restoring files on remote servers to a local device over a network comprising checking for an authentication code in the compressed bundle using the first cryptographic key. As indicated by the Examiner on page 5 of the Office Action dated July 13, 2006, Bailey does not expressly disclose the checking of an authentication code in the bundle using the first cryptographic key. However, the Examiner alleges that Matyas I teaches this limitation.

The Appellant respectfully submits that the Examiner has interpreted Matyas I too broadly and must look at Matyas I in its entirety. Matyas I teaches that the personal key client generates a MAC with ki, specifically MAC = Hash(file, ki). (See Matyas I, col. 12, ll. 1-7.) Matyas I further teaches that ki is a randomly generated integrity protection key generated by the personal key client. (See Matyas I, col. 9, ll. 23-30.) Therefore, in Matyas I, the MAC is created using a randomly generated encryption key.

In contrast, the Appellant's invention teaches checking of an authentication code in a bundle using the first cryptographic key. In other words, the authentication code is checked using a first cryptographic key that is derived from a user-provided passphrase. Therefore, unlike the Appellant's invention that teaches checking of an authentication code in a bundle using a first cryptographic key that is derived from a user-provided passphrase, Matyas I teaches that the MAC is created using an encryption key that is randomly generated by the personal key client.

Consequently, the Appellant respectfully submits that Bailey and Matyas I, alone or in any permissible combination, fail to teach or to suggest a method for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle using the first cryptographic key, as positively recited by Appellant's independent claim 5. Therefore, the Appellant respectfully submits that independent claim 5 fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

5. Claim 6

Claim 6 stands rejected under 35 U.S.C. §103 as being unpatentable over Bailey in view of Matyas I. Appellant respectfully traverses the rejection.

The Appellant submits that Bailey and Matyas I do not, in any permissible combination, teach, show, or suggest all of the limitations of independent claim 5. Since Bailey and Matyas I do not make obvious the Appellant's invention as recited in Appellant's independent claim 5, dependent claim 6 is also not made obvious since the claim depends directly from claim 5 and recites additional features of the present invention. Thus, claim 6 should be deemed patentable for at least the reasons stated above with respect to independent claim 5.

Secondly, the Appellant contends that the combination of Bailey and Matyas I does not teach the novel concept of a method for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle in combination with encrypting the bundle using a strong block cipher, as set forth in claim 6. Encrypting the bundle with a strong block cipher ensures greater security. This novel approach is absent in the alleged combination of Bailey with Matyas I. Thus, the Appellant respectfully submits that claim 6 is patentable under the provisions of 35 U.S.C. §103.

6. Claim 7

Claim 7 stands rejected under 35 U.S.C. §103 as being unpatentable over Bailey in view of Matyas I. Appellant respectfully traverses the rejection.

The Appellant submits that Bailey and Matyas I do not, in any permissible combination, teach, show, or suggest all of the limitations of independent claim 5. Since Bailey and Matyas I do not make obvious the Appellant's invention as recited in Appellant's independent claim 5, dependent claim 7 is also not made obvious since the claim depends directly from claim 5 and recites additional features of the present invention. Thus, claim 7 should be deemed patentable for at least the reasons stated above with respect to independent claim 5.

Secondly, the Appellant contends that the combination of Bailey and Matyas I does not teach the novel concept of a method for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle in combination with the authentication code being an HMAC, as set forth in claim 7. Using an HMAC as the authentication code ensures greater security. This novel approach is absent in the alleged combination of Bailey with Matyas I. Thus, the Appellant respectfully submits that claim 7 is patentable under the provisions of 35 U.S.C. §103.

7. Claim 9

The Examiner has rejected claim 9 in the Office Action under 35 U.S.C. §103 as being unpatentable over Bailey in view of Matyas I. Appellant respectfully traverses the rejection.

The teachings of Bailey and Matyas I are discussed above.

The Appellant respectfully submits that the combination of Bailey and Matyas I, alone or in any permissible combination, fails to teach or to suggest the novel concept of deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code for a bundle using the first cryptographic key that is ultimately added to and encrypted with the bundle, as positively claimed by the Appellant's independent claim 9. Specifically, Appellant's independent claim 9 positively recites:

> 9. A device-readable medium storing program instructions for performing a method of backing up one or more files on a local device onto remote servers over a network, the method comprising the steps of:
>
> deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;
>
> compressing one or more files and adding each of the files to a bundle;
>
> generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle; and
>
> encrypting the bundle using the second cryptographic key prior to sending the bundle to the remote server. (Emphasis added.)

In one embodiment, the Appellant's invention provides a device-readable medium storing program instructions for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle. The derivation step is performed after proactively checking the passphrase for a necessary amount of entropy. (See e.g., Appellant's specification, page 4, para. [0013].) In addition, due to the nature of how the bundle is constructed, the file system structure and the file names are advantageously hidden from the remote server and from anyone listening in on the network. (See *Id.* at page 6, para. [0016].) Consequently, the strong encryption and authentication properties make them tamper evident and opaque to anyone who cannot obtain a user passphrase or break the authentication and encryption files. (See *Id.* at page 7, para. [0020].)

The Appellant respectfully submits that the combination of Bailey and Matyas I, alone or in any permissible combination fails to teach or to suggest a device-readable medium storing program instructions for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase. Bailey explicitly teaches that "[t]he second encryption is performed by the transmission program based upon internally generated keys." (See Bailey, col. 17, ll. 14-16, emphasis added, see also, Bailey, col. 18, ll. 26-28, "while the second level of encryption is performed by the transmission program that generates its own key.", emphasis added.)

In addition, Bailey states that the client key is derived from a client selected string of characters and the actual encryption key used to encrypt the data is derived from the client key. In other words, the actual encryption key is not generated from the string of characters, but from the client key instead. (See Bailey Column 17, lines 1-5).

Matyas I fails to bridge the substantial gap left by Bailey because Matyas I teaches creating only one cryptographic key from a user-provided passphrase. (See Matyas I, col. 7, ll. 36-38; col. 9, ll. 15-23.) Unlike the Appellant's invention that teaches deriving a first cryptographic key **and** a second cryptographic key from a user-provided passphrase (i.e. both keys are derived from the user-provided passphrase), Matyas I teaches only one cryptographic key is generated based on a user provided passphrase and the additional cryptographic keys are randomly generated. (See *Id.*) As such, this element in Appellant's claims is completely absent in both references.

Moreover, as indicated by the Examiner on page 4 of the Office Action dated July 13, 2006, Bailey fails to disclose the generation of an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle. However, the Examiner alleges that Matyas I teaches this limitation.

The Appellant respectfully submits that the Examiner has interpreted Matyas I too broadly and must look at Matyas I in its entirety. Matyas I teaches that the personal key client generates a MAC with ki, specifically MAC = Hash(file, ki). (See Matyas I, col. 12, ll. 1-7.) Matyas I further teaches that ki is a randomly generated integrity protection key generated by the personal key client. (See Matyas I, col. 9, ll. 23-30.) Therefore, in Matyas I, the MAC is created using a randomly generated encryption key.

In contrast, the Appellant's invention teaches generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle. In other words, the authentication code is generated using a first cryptographic key that is derived from a user-provided passphrase. Therefore, unlike the Appellant's invention that teaches generating an authentication code using a first cryptographic key that is derived from a user-provided passphrase, Matyas I teaches that the MAC is created using an encryption key that is randomly generated by the personal key client.

Consequently, the Appellant respectfully submits that Bailey and Matyas I, alone or in any permissible combination, fail to teach or to suggest a device-readable medium storing program instructions for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle, as positively recited by Appellant's independent claim 9. Therefore, the Appellant respectfully submits that independent claim 9 fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

8. Claim 10

Claim 10 stands rejected under 35 U.S.C. §103 as being unpatentable over Bailey in view of Matyas I. Appellant respectfully traverses the rejection.

The Appellant submits that Bailey and Matyas I do not, in any permissible combination, teach, show, or suggest all of the limitations of independent claim 9. Since Bailey and Matyas I do not make obvious the Appellant's invention as recited in Appellant's independent claim 9, dependent claim 10 is also not made obvious since the claim depends directly from claim 9 and recites additional features of the present invention. Thus, claim 10 should be deemed patentable for at least the reasons stated above with respect to independent claim 9.

Secondly, the Appellant contends that the combination of Bailey and Matyas I does not teach the novel concept of a device-readable medium storing program instructions for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle in combination with encrypting the bundle using a strong block cipher, as set forth in claim 10. Encrypting the bundle with a strong block cipher ensures greater security. This novel approach is absent in the alleged combination of Bailey with Matyas I. Thus, the Appellant respectfully submits that claim 10 is patentable under the provisions of 35 U.S.C. §103.

9. Claim 11

Claim 11 stands rejected under 35 U.S.C. §103 as being unpatentable over Bailey in view of Matyas I. Appellant respectfully traverses the rejection.

The Appellant submits that Bailey and Matyas I do not, in any permissible combination, teach, show, or suggest all of the limitations of independent claim 9. Since Bailey and Matyas I do not make obvious the Appellant's invention as recited in Appellant's independent claim 9, dependent claim 11 is also not made obvious since the claim depends directly from claim 9 and recites additional features of the present invention. Thus, claim 11 should be deemed patentable for at least the reasons stated above with respect to independent claim 9.

Secondly, the Appellant contends that the combination of Bailey and Matyas I does not teach the novel concept of a device-readable medium storing program instructions for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle in combination with the authentication code being an HMAC, as set forth in claim 11. Using an HMAC as the authentication code ensures greater security. This novel approach is absent in the alleged combination of Bailey with Matyas I. Thus, the Appellant respectfully submits that claim 11 is patentable under the provisions of 35 U.S.C. §103.

10. Claim 13

The Examiner has rejected claim 13 in the Office Action under 35 U.S.C. §103 as being unpatentable over Bailey in view of Matyas I. Appellant respectfully traverses the rejection.

The teachings of Bailey and Matyas I are discussed above

The Appellant respectfully submits that the combination of Bailey and Matyas I, alone or in any permissible combination, fails to teach or to suggest the novel concept of deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle using the first cryptographic key, as positively claimed by the Appellant's independent claim 13. Specifically, Appellant's independent claim 13 positively recites:

> 13. A device-readable medium storing program instructions for performing a method of restoring one or more files on remote servers to a local device over a network, the method comprising the steps of:
> provided passphraase;
> decrypting a bundle received from the remote server using the second cryptographic key;
> checking an authentication code in the bundle using the first cryptographic key; and
> decompressing one or more files from the bundle. (Emphasis added.)

In one embodiment, the Appellant's invention provides a device-readable medium storing program instructions for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle using the first cryptographic key. The derivation step is performed after proactively checking the passphrase for a necessary amount of entropy. (See e.g., Appellant's specification, page 4, para. [0013].) In addition, due to the nature of how the bundle is constructed, the file system structure and the file names are advantageously hidden from the remote server and from anyone listening in on the network. (See *Id.* at page 6, para. [0016].) Consequently, the strong encryption and authentication properties make them tamper evident and opaque to anyone who cannot obtain a user passphrase or break the authentication and encryption files. (See *Id.* at page 7, para. [0020].)

The Appellant respectfully submits that the combination of Bailey and Matyas I, alone or in any permissible combination fails to teach or to suggest a device-readable medium storing program instructions for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase. Bailey explicitly teaches that "[t]he second encryption is performed by the transmission program based upon internally generated keys." (See Bailey, col. 17, ll. 14-16, emphasis added, see also, Bailey, col. 18, ll. 26-28, "while the second level of encryption is performed by the transmission program that generates its own key.", emphasis added.)

In addition, Bailey states that the client key is derived from a client selected string of characters and the actual encryption key used to encrypt the data is derived from the client key. In other words, the actual encryption key is not generated from the string of characters, but from the client key instead. (See Bailey Column 17, lines 1-5).

Matyas I fails to bridge the substantial gap left by Bailey because Matyas I teaches creating only one cryptographic key from a user-provided passphrase. (See Matyas I, col. 7, ll. 36-38; col. 9, ll. 15-23.) Unlike the Appellant's invention that teaches deriving a first cryptographic key **and** a second cryptographic key from a user-provided passphrase (i.e. both keys are derived from the user-provided passphrase), Matyas I teaches only one cryptographic key is generated based on a user provided passphrase and the additional cryptographic keys are randomly generated. (See *Id.*) As such, this element in Appellant's claims is completely absent in both references.

Appellant also respectfully submits that the combination of Bailey and Matyas I, alone or in any permissible combination fails to teach or to suggest a method for restoring files on remote servers to a local device over a network comprising checking for an authentication code in the compressed bundle using the first cryptographic key. As indicated by the Examiner on page 5 of the Office Action dated July 13, 2006, Bailey does not expressly disclose the checking of an authentication code in the bundle using the first cryptographic key. However, the Examiner alleges that Matyas I teaches this limitation.

The Appellant respectfully submits that the Examiner has interpreted Matyas I too broadly and must look at Matyas I in its entirety. Matyas I teaches that the personal key client generates a MAC with ki, specifically MAC = Hash(file, ki). (See Matyas I, col. 12, ll. 1-7.) Matyas I further teaches that ki is a randomly generated integrity protection key generated by the personal key client. (See Matyas I, col. 9, ll. 23-30.) Therefore, in Matyas I, the MAC is created using a randomly generated encryption key.

In contrast, the Appellant's invention teaches checking of an authentication code in a bundle using the first cryptographic key. In other words, the authentication code is checked using a first cryptographic key that is derived from a user-provided passphrase. Therefore, unlike the Appellant's invention that teaches checking of an authentication code in a bundle using a first cryptographic key that is derived from a user-provided passphrase, Matyas I teaches that the MAC is created using an encryption key that is randomly generated by the personal key client.

Consequently, the Appellant respectfully submits that Bailey and Matyas I, alone or in any permissible combination, fail to teach or to suggest a device-readable medium storing program instructions for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle using the first cryptographic key, as positively recited by Appellant's independent claim 13. Therefore, the Appellant respectfully submits that independent claim 13 fully satisfies the requirements of 35 U.S.C. § 103 and is patentable thereunder.

11. Claim 14

Claim 14 stands rejected under 35 U.S.C. §103 as being unpatentable over Bailey in view of Matyas I. Appellant respectfully traverses the rejection.

The Appellant submits that Bailey and Matyas I do not, in any permissible combination, teach, show, or suggest all of the limitations of independent claim 13. Since Bailey and Matyas I do not make obvious the Appellant's invention as recited in Appellant's independent claim 13, dependent claim 14 is also not made obvious since the claim depends directly from claim 13 and recites additional features of the present invention. Thus, claim 14 should be deemed patentable for at least the reasons stated above with respect to independent claim 13.

Secondly, the Appellant contends that the combination of Bailey and Matyas I does not teach the novel concept of a device-readable medium storing program instructions for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle in combination with encrypting the bundle using a strong block cipher, as set forth in claim 14. Encrypting the bundle with a strong block cipher ensures greater security. This novel approach is absent in the alleged combination of Bailey with Matyas I. Thus, the Appellant respectfully submits that claim 14 is patentable under the provisions of 35 U.S.C. §103.

12. Claim 15

Claim 15 stands rejected under 35 U.S.C. §103 as being unpatentable over Bailey in view of Matyas I. Appellant respectfully traverses the rejection.

The Appellant submits that Bailey and Matyas I do not, in any permissible combination, teach, show, or suggest all of the limitations of independent claim 13. Since Bailey and Matyas I do not make obvious the Appellant's invention as recited in Appellant's independent claim 13, dependent claim 15 is also not made obvious since the claim depends directly from claim 13 and recites additional features of the present invention. Thus, claim 15 should be deemed patentable for at least the reasons stated above with respect to independent claim 13.

Secondly, the Appellant contends that the combination of Bailey and Matyas I does not teach the novel concept of a device-readable medium storing program instructions for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle in combination with the authentication code being an HMAC, as set forth in claim 15. Using an HMAC as the authentication code ensures greater security. This novel approach is absent in the alleged combination of Bailey with Matyas I. Thus, the Appellant respectfully submits that claim 15 is patentable under the provisions of 35 U.S.C. §103.

B. 35 U.S.C. §103(a) – Bailey and Matyas I in view of Matyas II

1. Claim 4

The Examiner has rejected claim 4 in the Office Action under 35 U.S.C. § 103 as being unpatentable over Bailey in view of Matyas I, and in further view of Matyas II. Appellant respectfully traverses the rejection.

The teachings of Bailey and Matyas I have been discussed above. Matyas II teaches a method for generating public and private key pairs without using a passphrase. (See Matyas II, Title and Abstract, emphasis added).

As discussed above with respect to Appellant's independent claim 1, the combination of Bailey and Matyas I fails to teach, show or suggest the Appellant's invention. Specifically, Bailey and Matyas I fail to disclose the novel concept of a method for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle. (See Appellant's claim 1, *supra*). Furthermore, Matyas II fails to bridge the substantial gap left by Bailey and Matyas I. Matyas II directly teaches away from the Appellant's invention because Matyas II explicitly teaches a method for generating public and private key pairs without using a passphrase. (See Matyas II, Title, and Abstract, emphasis added).

Since Bailey in view of Matyas I, and in further view of Matyas II do not make obvious the Appellant's invention as recited in Appellant's independent claim 1, dependent claim 4 is also not made obvious since the claim depends directly from claim 1 and recites additional features of the present invention. Thus, claim 4 should be deemed patentable for at least the reasons stated above with respect to independent claim 1.

Secondly, the Appellant contends that the combination of Bailey, Matyas I and Matyas II does not teach the novel concept of a method for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle in combination with the cryptographic keys containing at least 128 bits, as set forth in claim 4. Cryptographic keys containing at least 128 bits ensures greater security. This novel approach is absent in the alleged combination of Bailey and Matyas I with Matyas II. Thus, the Appellant respectfully submits that claim 4 is patentable under the provisions of 35 U.S.C. §103.

2. Claim 8

The Examiner has rejected claim 8 in the Office Action under 35 U.S.C. § 103 as being unpatentable over Bailey in view of Matyas I, and in further view of Matyas II. Appellant respectfully traverses the rejection.

The teachings of Bailey and Matyas I have been discussed above. Matyas II teaches a method for generating public and private key pairs without using a passphrase. (See Matyas II, Title and Abstract, emphasis added).

As discussed above with respect to Appellant's independent claim 5, the combination of Bailey and Matyas I fails to teach, show or suggest the Appellant's invention. Specifically, Bailey and Matyas I fail to disclose the novel concept of a method for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle using the first cryptographic key. (See Appellant's claim 5, *supra*). Furthermore, Matyas II fails to bridge the substantial gap left by Bailey and Matyas I. Matyas II directly teaches away from the Appellant's invention because Matyas II explicitly teaches a method for generating public and private key pairs without using a passphrase. (See Matyas II, Title, and Abstract, emphasis added).

Since Bailey in view of Matyas I, and in further view of Matyas II do not make obvious the Appellant's invention as recited in Appellant's independent claim 5, dependent claim 8 is also not made obvious since the claim depends directly from claim 5 and recites additional features of the present invention. Thus, claim 8 should be deemed patentable for at least the reasons stated above with respect to independent claim 5.

Secondly, the Appellant contends that the combination of Bailey, Matyas I and Matyas II does not teach the novel concept of a method for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle in combination with the cryptographic keys containing at least 128 bits, as set forth in claim 8. Cryptographic keys containing at least 128 bits ensures greater security. This novel approach is absent in the alleged combination of Bailey and Matyas I with Matyas II. Thus, the Appellant respectfully submits that claim 8 is patentable under the provisions of 35 U.S.C. §103.

3. Claim 12

The Examiner has rejected claim 12 in the Office Action under 35 U.S.C. § 103 as being unpatentable over Bailey in view of Matyas I, and in further view of Matyas II. Appellant respectfully traverses the rejection.

The teachings of Bailey and Matyas I have been discussed above. Matyas II teaches a method for generating public and private key pairs without using a passphrase. (See Matyas II, Title, and Abstract, emphasis added).

As discussed above with respect to Appellant's independent claim 9, the combination of Bailey and Matyas I fails to teach, show or suggest the Appellant's invention. Specifically, Bailey and Matyas I fail to disclose the novel concept of a device-readable medium storing program instructions for backing up files from a local device onto remote servers over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle. (See Appellant's claim 9, *supra*). Furthermore, Matyas II fails to bridge the substantial gap left by Bailey and Matyas I. Matyas II directly teaches away from the Appellant's invention because Matyas II explicitly teaches a method for generating public and private key pairs without using a passphrase. (See Matyas II, Title and Abstract, emphasis added).

Since Bailey in view of Matyas I, and in further view of Matyas II do not make obvious the Appellant's invention as recited in Appellant's independent claim 9, dependent claim 12 is also not made obvious since the claim depends directly from claim 9 and recites additional features of the present invention. Thus, claim 12 should be deemed patentable for at least the reasons stated above with respect to independent claim 9.

Secondly, the Appellant contends that the combination of Bailey, Matyas I and Matyas II does not teach the novel concept of a device-readable medium storing program instructions for backing up files from a local device onto remote servers over a network comprising <u>deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase</u> and <u>generating an authentication code using the first cryptographic key for a bundle that is ultimately added to and encrypted with the bundle</u> in combination with the cryptographic keys containing at least 128 bits, as set forth in claim 12. Cryptographic keys containing at least 128 bits ensures greater security. This novel approach is absent in the alleged combination of Bailey and Matyas I with Matyas II. Thus, the Appellant respectfully submits that claim 12 is patentable under the provisions of 35 U.S.C. §103.

4. <u>Claim 16</u>

The Examiner has rejected claim 16 in the Office Action under 35 U.S.C. § 103 as being unpatentable over Bailey in view of Matyas I, and in further view of Matyas II. Appellant respectfully traverses the rejection.

The teachings of Bailey and Matyas I have been discussed above. Matyas II teaches a method for generating public and private key pairs <u>without using a passphrase</u>. (See Matyas II, Title, and Abstract, emphasis added).

As discussed above with respect to Appellant's independent claim 13, the combination of Bailey and Matyas I fails to teach, show or suggest the Appellant's invention. Specifically, Bailey and Matyas I fail to disclose the novel concept of a device-readable medium storing program instructions for restoring files on remote servers to a local device over a network comprising <u>deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase</u> and <u>checking for an authentication code in the compressed bundle using the first cryptographic key</u>. (See Appellant's claim 13, *supra*). Furthermore, Matyas II fails to bridge the substantial gap left by Bailey and Matyas I. Matyas II directly teaches away from the Appellant's invention because Matyas II explicitly teaches a method for generating public and private key pairs without using a passphrase. (See Matyas II, Title, and Abstract, emphasis added).

Since Bailey in view of Matyas I, and in further view of Matyas II do not make obvious the Appellant's invention as recited in Appellant's independent claim 13, dependent claim 16 is also not made obvious since the claim depends directly from claim 13 and recites additional features of the present invention. Thus, claim 16 should be deemed patentable for at least the reasons stated above with respect to independent claim 13.

Secondly, the Appellant contends that the combination of Bailey, Matyas I and Matyas II does not teach the novel concept of a device-readable medium storing program instructions for restoring files on remote servers to a local device over a network comprising deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase and checking for an authentication code in the compressed bundle using the first cryptographic key in combination with the cryptographic keys containing at least 128 bits, as set forth in claim 16. Cryptographic keys containing at least 128 bits ensures greater security. This novel approach is absent in the alleged combination of Bailey and Matyas I with Matyas II. Thus, the Appellant respectfully submits that claim 16 is patentable under the provisions of 35 U.S.C. §103.

CONCLUSION

For the reasons advanced above, the Appellant respectfully urges that the rejections of claims 1-16 as being unpatentable under 35 U.S.C. §103 are improper. Reversal of the rejections in this appeal is respectfully requested. If necessary, please charge any shortage in fees due in connection with the filing of this paper, including extension of time fees or the difference in fees previously paid for the Notice of Appeal and the Appeal Brief, to Deposit Account No. 20-0782/ATT2000-0415, and please credit any excess fees to the above referenced deposit account.

Respectfully submitted,

October 13, 2006

Kin-Wah Tong
Attorney Reg. No. 39,400
(732) 530-9404

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Suite 100
Shrewsbury, NJ 07702

CLAIMS APPENDIX

1. (Original) A method of backing up one or more files on a local device onto remote servers over a network comprising:

deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;

compressing one or more files and adding each of the files to a bundle;

generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle; and

encrypting the bundle using the second cryptographic key prior to sending the bundle to the remote server.

2. (Original) The invention of claim 1 wherein the bundle is encrypted using a strong block cipher.

3. (Original) The invention of claim 1 wherein the authentication code is an HMAC.

4. (Original) The invention of claim 1 wherein the cryptographic keys contain at least 128 bits.

5. (Previously Presented) A method of restoring one or more files on remote servers to a local device over a network comprising:

deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;

decrypting a bundle received from the remote server using the second cryptographic key;

checking an authentication code in the bundle using the first cryptographic key; and

decompressing one or more files from the bundle.

6. (Original) The invention of claim 5 wherein the bundle was encrypted using a strong block cipher.

7. (Original) The invention of claim 5 wherein the authentication code is an HMAC.

8. (Original) The invention of claim 5 wherein the cryptographic keys contain at least 128 bits.

9. (Original) A device-readable medium storing program instructions for performing a method of backing up one or more files on a local device onto remote servers over a network, the method comprising the steps of:

deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;

compressing one or more files and adding each of the files to a bundle;

generating an authentication code for the bundle using the first cryptographic key and adding the authentication code to the bundle; and

encrypting the bundle using the second cryptographic key prior to sending the bundle to the remote server.

10. (Original) The invention of claim 9 wherein the bundle is encrypted using a strong block cipher.

11. (Original) The invention of claim 9 wherein the authentication code is an HMAC.

12. (Original) The invention of claim 9 wherein the cryptographic keys contain at least 128 bits.

13. (Previously Presented) A device-readable medium storing program instructions for performing a method of restoring one or more files on remote servers to a local device over a network, the method comprising the steps of:

deriving a first cryptographic key and a second cryptographic key from a user-provided passphrase;

decrypting a bundle received from the remote server using the second cryptographic key;

checking an authentication code in the bundle using the first cryptographic key;

and

decompressing one or more files from the bundle.

14. (Original) The invention of claim 13 wherein the bundle was encrypted using a strong block cipher.

15. (Original) The invention of claim 13 wherein the authentication code is an HMAC.

16. (Original) The invention of claim 13 wherein the cryptographic keys contain at least 128 bits.

EVIDENCE APPENDIX

None

RELATED PROCEEDINGS APPENDIX

None